Hypotheses testing for maximally entangled state (Statistical Inference of Records and Related Statistics)

AUTHOR(S):

Hayashi, Masahito

数理解析研究所講究録 1439 巻 2005 年 225-240

Hypotheses testing for maximally entangled state

Masahito Hayashi[1,*]

[1]*Quantum Computation and Information Project, ERATO, JST*
5-28-3, Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan
Superrobust Computation Project, Information Science and Technology Strategic Core (21st Century COE by MEXT)
Graduate School of Information Science and Technology, The University of Tokyo
7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan

In the asymptotic setting, the optimal test for hypotheses tesing of the maximally entangled state is derived under several locality conditions for measurements. The optimal test is obtained in several special cases with finite samples. In addition, the experimental scheme for the optimal test is presented.

PACS numbers: 03.65.Wj,03.65.Ud,02.20.-a

I. INTRODUCTION

Recently various quantum information processings are proposed, and many of them require maximally entangled states as resources[6, 7, 9]. Hence, it is often desired to generate maximally entangled states experimentally. In particular, it must be based on statistical method to decide whether the state generated experimentally is really the required maximally entangled state.

Now, entanglement witness is often used as its standard method [14, 19]. It is, however, not necessarily the optimal method from a viewpoint of statistics. On the other hand, in mathematical statistics, the decision problem of the truth of the given hypothesis is called statistical hypothesis testing, and is systematically studied. Hence, it is desired to treat, under the frame of statistical hypotheses testing, the problem deciding whether the given quantum state is the required maximally entangled state. In statistical hypotheses testing, we suppose two hypotheses (null hypothesis and alternative hypothesis) to be tested a priori, and assume that one of both is true. Based on observed data, we decide which hypothesis is true. Most preceding studies about quantum hypotheses testing concerned only quantum Neymann Pearson lemma [3, 12] and quantum Stein's lemma[11, 13, 20], except Tsuda *et al.* [1]. In these settings, they treated the case when both of the null and the alternative hypotheses consist of a single quantum state, *i.e.*, they are simple.

However, in our issue, it is unnatural to specify both hypotheses with one quantum state. Hence, we cannot directly apply quantum Neymann Pearson theorem and quantum Stein's lemma, and we have to treat composite hypotheses, *i.e.*, the case where both hypotheses consist of multiple quantum states. It is also required to restrict our measurements for testing among measurements based on LOCC (local operations and classical communications) because the tested state is maximally entangled state.

Recently, based on quantum statistical inference[3, 4, 12], Tsuda *et al.*[1] discussed this testing problem under statistical hypotheses testing. They treated testing problem where the null hypothesis consists only of the required maximally entangled state. Especially, they studied the optimal test and the existence of the uniformally optimal test (whose definition will be presented later) when one or two samples of the state to be tested are given. Their analysis mainly concentrated the two-dimensional case.

In this paper, we treat the null hypothesis consisting of quantum states whose fidelity for the desired maximally entangled state is less than ϵ, and discuss this testing problem with several given samples of the tested state in the following three setting concerning the range of our measurements. **M1**: All measurements are allowed. **M2**: Only classical communications are allowed as our operations between two distinct parties, but any operations among samples are available. **M3**: As well as measuring apparatus with quantum correlation between two distinct parties, those with quantum correlation among local samples are forbidden. The restriction **M3** for measurement is discussed by Virmani and Plenio [21], the first time. Tsuda *et al.*[1] treated the settings **M2** and **M3**, more systematically.

This paper mainly treats the case of sufficiently many samples, *i.e.*, first order asymptotic theory. As a result, we find that there is no difference in performances of both settings **M1** and **M2**. Especially, the test achieving the asymptotical optimal performance can be realized by quantum measurement with quantum correlations between only two local samples. That is, even if we use any higher quantum correlations among local samples, no further improvement is available under the first order asymptotic frame work. In the two-dimensional case, the required measurement with local quantum correlations is the four-valued Bell measurement between the local two samples. In the setting **M3**, we treat the null hypothesis consisting only of the maximally entangled state. Then, it is proved that even if we use classical correlation between local samples for deciding local measurement, there is no further improvement. That is, it

*Electronic address: masahito@qci.jst.go.jp

is optimal to repeat the optimal measurement in the one sample case in the setting **M3**.

Concerning non-asymptotic setting, we derive the optimal test with arbitrary finite number of samples under a suitable group symmetry. This result can be trivially extended to hypothesis testing of arbitrary pure state. Moreover, we derive the optimal test with two samples under the several conditions, and calculate its optimal performance.

Furthermore, we treat the case when two or three different quantum states are prepared, and obtain the optimal test with one sample in both settings **M2** and **M3**. (In this assumption, even if the number of samples is one, every party consists of multiple systems. Hence, the setting **M2** means the setting where the quantum correlation among these system are available in the measuring apparatus, and the setting **M3** means the setting where such a correlation is forbidden in the measuring apparatus. It is proved that repeating the optimal measurement for one sample gives the test achieving the asymptotically optimal performance. Moreover, it is shown that for this purpose, we can replace the optimal measurement of one sample by four-valued Bell measurement in the two-state case. (Indeed, it is difficult to perform the quantum measurement with quantum correlation between two samples because we need to prepare two samples at the same time. Hence, it is easier to realize quantum measurement with one sample of two different quantum states.) In the three states case, the optimal measurement can be described by the GHZ state $\frac{1}{\sqrt{d}}\sum_i |i\rangle|i\rangle|i\rangle$, where d is the dimension of the system. This fact seems to indicate the importance of the GHZ state in the three parties.

Concerning locality restriction of our measurement, it is natural to treat two-way LOCC, but we treat one-way LOCC and separable measurement. This is because the separability condition is easier to treat than two-way LOCC. Hence, this paper mainly adopts separability as a useful mathematical condition. It is contrast that Virmani and Plenio[21] used the PPT condition and Tsuda *et al.*[1] partially used the PPT condition.

This paper is organized as follows. The mathematical formulation of statistical hypotheses testing is given in section II and, the group theoretical symmetry is explained in section III B. In section III C, we explain the restrictions of our measurement for our testing, for example, one-way LOCC, two-way LOCC, separability, *etc.* In section IV, we review the fundamental knowledge of statistical hypotheses testing for the probability distributions as preliminary. In section V(section VI, section VII), the setting **M1**(**M2**, **M3**) is discussed, respectively. Further results in the two-dimensional case are presented in section VIII. Finally, in section IX (section X), we discuss the case of two (three) different quantum states, respectively. All proofs are omitted because of the limit of the page.

II. MATHEMATICAL FORMULATION OF QUANTUM HYPOTHESIS TESTING

Let $\mathcal{H}$ be a finite-dimensional Hilbert space corresponding to the physical system of interest. Then, the state is described by a density matrix on $\mathcal{H}$. In the quantum hypothesis testing, we assume that the current state ρ of the system is unknown, but is known to belong to a subset $\mathcal{S}_0$ or $\mathcal{S}_1$ of the set of densities. Hence, our task is testing

$$H_0 : \rho \in \mathcal{S}_0 \quad \text{versus} \quad H_1 : \rho \in \mathcal{S}_1 \tag{1}$$

based on an appropriate measurement on $\mathcal{H}$. That is, we are required to decide which hypothesis is true. We call H_0 *a null hypothesis*, and we call H_1 *an alternative hypothesis*.

A test for the hypothesis (1) is given by a Positive Operator Valued Measure (POVM) $\{T_0, T_1\}$ on $\mathcal{H}$ composed of two elements, where $T_0 + T_1 = I$. For simplicity, the test $\{T_0, T_1\}$ is described by the operator $T = T_0$. Our decision should be done based on this test as follows: We accept H_0 (=we reject H_1) if we observe T_0, and we accept H_1 (=we reject H_0) if we observe T_1. In order to treat its performance, we focus on the following two kinds of errors.: A type 1 error is an event such that we accept H_1 though H_0 is true. A type 2 error is an event such that we accept H_0 though H_1 is true. Hence, we treat the following two kinds of error probabilities: The type 1 error probability $\alpha(T, \rho)$ and the type 2 error probabilities $\beta(T, \rho)$ are given by

$$\alpha(T, \rho) = \mathrm{Tr}(\rho T_1) = 1 - \mathrm{Tr}(\rho T) \ (\rho \in \mathcal{S}_0),$$
$$\beta(T, \rho) = \mathrm{Tr}(\rho T_0) = \mathrm{Tr}(\rho T) \ (\rho \in \mathcal{S}_1).$$

A quantity $1 - \beta(T, \rho)$ is called *power*. A test T is said to be *level-*α if $\alpha(T, \rho) \le \alpha$ for any $\rho \in \mathcal{S}_0$.

In hypothesis testing, we restrict our test to tests whose first error probability is greater than a given constant α for any element $\rho \in \mathcal{S}_0$. That is, since the type 1 error is considered to be more serious than the type 2 error in hypothesis testing, it is required to guarantee that the type 1 error probability is less than a constant which is called level of significance or level. Hence, a test T is said to be *level-*α if $\alpha(T, \rho) \le \alpha$ for any $\rho \in \mathcal{S}_0$.

Then, under this condition, the performance of the test is given by $1 - \beta(T, \rho)$ for $\rho \in \mathcal{S}_1$, which is called *power*. Therefore, we often optimize the type 2 error probability as follows:

$$\beta_\alpha(\mathcal{S}_0 \| \rho) \stackrel{\mathrm{def}}{=} \min_{T \in \mathcal{T}_{\alpha,\mathcal{S}_0}} \beta(T, \rho),$$

$$\mathcal{T}_{\alpha,\mathcal{S}_0} \stackrel{\mathrm{def}}{=} \{T | 0 \le T \le I, \quad \alpha(T, \rho) \le \alpha \forall \rho \in \mathcal{S}_0\}$$

for any $\rho \in \mathcal{S}_1$. Especially, a test $T \in \mathcal{T}_{\alpha,\mathcal{S}_0}$ is called *a Most Powerful (MP) test with level* α *at* $\rho \in \mathcal{S}_1$ if $\beta(T, \rho) \le \beta(T', \rho)$ for any level-α test $T' \in \mathcal{T}_{\alpha,\mathcal{S}_0}$, that is,

$$\beta(T, \rho) = \beta_\alpha(\mathcal{S}_0 \| \rho).$$

Moreover, a test $T \in \mathcal{T}_{\alpha,\mathcal{S}_0}$ is called *a Uniformly Most Powerful (UMP) test* if T is MP for any level-α test $\rho \in \mathcal{S}_1$, that is,

$$\beta(T,\rho) = \beta_\alpha(\mathcal{S}_0\|\rho), \quad \forall \rho \in \mathcal{S}_1.$$

However, in certain instances, it is natural to restrict our testings to those satisfying one or two conditions (C_1 or C_1 and C_2). In such a case, we focus on the following quantity in stead of $\beta(T,\rho)$:

$$\beta^{C_2}_{\alpha,C_1}(S_0\|\rho) \stackrel{\rm def}{=} \min_{T\in\mathcal{T}_{\alpha,\mathcal{S}_0}} \{\beta(T,\rho)|T \text{ satisfies } C_1 \text{ and } C_2.\}.$$

If a test $T \in\in \mathcal{T}_{\alpha,\mathcal{S}_0}$ satisfies conditions C_1, C_2, and

$$\beta(T,\rho) = \beta^{C_2}_{\alpha,C_1}(\mathcal{S}_0\|\rho), \quad \forall \rho \in \mathcal{S}_1,$$

it is called *a Uniformly Most Powerful C_1, C_2 (UMP C_1, C_2) test.*

be T.

III. OUR PROBLEMS

A. Hypothesis

Our problem in this article is the hypothesis testing of the maximal entangled state

$$|\phi^0_{AB}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_B$$

on the tensor product space $\mathcal{H}_{A,B}$ of the two d-dimensional systems $\mathcal{H}_A$ and $\mathcal{H}_B$ spanned by $|0\rangle_A, |1\rangle_A, ..., |d-1\rangle_A$ and $|0\rangle_B, |1\rangle_B, ..., |d-1\rangle_B$, respectively. Note that we refer to $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ as *the standard basis.* Suppose that n independent samples are provided, that is, the state is given in the form

$$\rho = \bigotimes_{i=1}^n \sigma_i = \underbrace{\sigma_1 \otimes \cdots \otimes \sigma_n}_{n}$$

for n unknown densities $\sigma_1, \ldots \sigma_n$. We also assume that these densities $\sigma_1, \ldots, \sigma_n$ equal a density σ. In this case, the state ρ is called *n-independent and identical density (n-i.i.d.).* In the following, we consider two settings for our hypotheses:

$$H_0: \ \sigma \in \mathcal{S}_{\le\epsilon} \stackrel{\rm def}{=} \{\sigma | 1 - \langle\phi^0_{AB}|\sigma|\phi^0_{AB}\rangle \le \epsilon\}$$
versus
$$H_1: \ \sigma \in \mathcal{S}^{\rm c}_{\le\epsilon}$$

and

$$H_0: \ \sigma \in \mathcal{S}_{\ge\epsilon} \stackrel{\rm def}{=} \{\sigma | 1 - \langle\phi^0_{AB}|\sigma|\phi^0_{AB}\rangle \ge \epsilon\}$$
versus
$$H_1: \ \sigma \in \mathcal{S}^{\rm c}_{\ge\epsilon}.$$

When the null hypothesis is "$\sigma \in \mathcal{S}_{\le\epsilon}$", the set of level α-tests is given in the n-fold i.i.d. case by

$$\mathcal{T}^n_{\alpha,\le\epsilon} \stackrel{\rm def}{=} \left\{T \middle| 0 \le T \le I, \quad \forall\sigma \in \mathcal{S}_{\le\epsilon}, \ 1 - {\rm Tr}\,\sigma^{\otimes n} T \le \alpha\right\}.$$

Similarly, when the null hypothesis is "$\sigma \in \mathcal{S}_{\ge\epsilon}$", the set of level α-tests is given in the n-fold i.i.d. case by

$$\mathcal{T}^n_{\alpha,\ge\epsilon} \stackrel{\rm def}{=} \left\{T \middle| 0 \le T \le I, \quad \forall\sigma \in \mathcal{S}_{\ge\epsilon}, \ 1 - {\rm Tr}\,\sigma^{\otimes n} T \le \alpha\right\}.$$

In this paper, we only treat the null hypothesis $\mathcal{S}_{\le\epsilon}$. However, a large part of obtained results can be trivially extended to the case of the null hypothesis $\mathcal{S}_{\ge\epsilon}$.

B. Restriction I: group action

In this paper, we treat these two cases with the invariance conditions for the following group action, which preserve the two hypotheses H_0 and H_1. The naturalness of this condition will be discussed later.

1)$U(1)$-action:

$$\phi \mapsto U_0\phi, \quad \phi \in \mathcal{H}_{A,B}, \quad \theta \in \mathbb{R}$$

where U_θ is defined by

$$U_\theta \stackrel{\rm def}{=} e^{i\theta}|\phi^0_{AB}\rangle\langle\phi^0_{AB}| + (I - |\phi^0_{AB}\rangle\langle\phi^0_{AB}|).$$

For a vector $|u\rangle$ orthogonal to $\langle\phi^0_{AB}|$ and a positive number $0 < p < 1$, the entanglement properties of the two sates $\sqrt{p}|\phi^0_{AB}\rangle + \sqrt{1-p}|u\rangle$ and $e^{i\theta}\sqrt{p}|\phi^0_{AB}\rangle + \sqrt{1-p}|u\rangle$ are essentially equivalent. Hence, this symmetry is very natural. We can easily check that this action preserves our hypotheses. The $U(1)$-action is so small that it is not suitable to adopt this invariance as our restriction. However, this invariance can be, often, treated so easily that it be adopted only by a technical reason.

2)$SU(d)$-action: We consider the unitary action on the tensor product space $\mathcal{H}_{A,B} = \mathcal{H}_A \otimes \mathcal{H}_B$:

$$\phi \mapsto U(g)\phi, \quad \phi \in \mathcal{H}_{A,B}, \quad g \in SU(d),$$

where

$$U(g) \stackrel{\rm def}{=} g \otimes \overline{g},$$

and $\overline{g}$ is the complex conjugate of g concerning the standard basis $|0\rangle_B, |1\rangle_B, ..., |d-1\rangle_B$ on the system B. Indeed, this action preserves the maximally entangled state $|\phi^0_{AB}\rangle$. Hence, this action preserves our hypotheses. Furthermore, this action preserves the entanglement property. Similarly to the $U(1)$-invariance, the $SU(1)$-action is so small that it will be adopted only by a technical reason.

3)$SU(d) \times U(1)$-action: Since the $SU(d)$ action and the $U(1)$-action preserve the entanglement property, the following action of the direct sum product group $SU(d) \times U(1)$ of $SU(d)$ and $U(1)$ also preserves this property:

$$\phi \mapsto U(g,\theta)\phi \quad \phi \in \mathcal{H}_{A,B}, \quad (g, e^{i\theta}) \in SU(d) \times U(1),$$

where

$$U(g,\theta) \stackrel{\rm def}{=} U(g)U_\theta = U_\theta U(g).$$

Thus, this condition is most suitable as our restriction.

4)$U(d^2-1)$-action: As a stronger invariance, we can consider the invariance of the $U(d^2-1)$-action, *i.e.*, the following unitary action on the orthogonal space of $|\phi^0_{AB}\rangle\langle\phi^0_{AB}|$, which is a d^2-1-dimensional space.

$$\phi \mapsto V(g)\phi, \quad \phi \in \mathcal{H}_{A,B}, \quad g \in U(d^2-1).$$

where

$$V(g) \stackrel{\rm def}{=} g(I - |\phi^0_{AB}\rangle\langle\phi^0_{AB}|) + |\phi^0_{AB}\rangle\langle\phi^0_{AB}|.$$

This group action contains the $U(1)$-action and the $SU(d)$-action. Hence, the invariance of the $U(d^2-1)$-action is stronger than the invariances of above three actions. This action does not preserve the entanglement property. Thus, based on this definition, we cannot say that this condition is natural for our setting while it is natural if we are not care of entanglement.

Furthermore, in the n-fold i.i.d. setting, it is suitable to assume the invariance of the n-tensor product action of the above actions, *i.e.*, $U_\theta^{\otimes n}$, $U(g)^{\otimes n}$, $U(g,\theta)^{\otimes n}$, $V(g)^{\otimes n}$, *etc.*

C. Restriction II: locality

When the system consists of two distinct parties A and B, it is natural to restrict our testing to LOCC measurements between A and B. Hence, we can consider several restrictions concerning locality condition. Hence, in section IV, as the first step, in order to discuss the hypotheses testing with the null hypothesis $\mathcal{S}_{\le\epsilon}$, we will treat the following optimization:

$$\beta^n_{\alpha,G}(\le \epsilon\|\sigma) \stackrel{\rm def}{=} \min_{T\in T^n_{\alpha,\le\epsilon}} \left\{\beta(T,\sigma^{\otimes n}) \,|T \text{ is } G\text{-invariant.}\right\},$$

where $G = U(1), SU(d), SU(d)\times U(1)$, or $U(d^2-1)$. However, since our quantum system consists of two distant system, we cannot neccessarily use all measurements. Hence, it is natural to restrict our test to a class of tests. In this paper, we focus on the following seven classes.

$\emptyset$: No condition

$S(A,B)$: The test is *separable* between two systems $\mathcal{H}_A^{\otimes n}$ and $\mathcal{H}_B^{\otimes n}$, *i.e.*, the test T has the following form:

$$T = \sum_i a_i T_i^A \otimes T_i^B,$$

where $a_i \ge 0$ and the matrix T_i^A (T_i^B) is a positive semi-definite matrix on the system $\mathcal{H}_A^{\otimes n}$ ($\mathcal{H}_B^{\otimes n}$), respectively.

$L(A \leftrightarrows B)$: The test can be realized by two-way LOCC between two systems $\mathcal{H}_A^{\otimes n}$ and $\mathcal{H}_B^{\otimes n}$.

$L(A \to B)$: The test can be realized by one-way LOCC from the system $\mathcal{H}_A^{\otimes n}$ to the system $\mathcal{H}_B^{\otimes n}$.

$S(A_1,\ldots,A_n,B_1,\ldots,B_n)$: The test is separable among $2n$ systems $\mathcal{H}_{A_1},\ldots,\mathcal{H}_{A_n},\mathcal{H}_{B_1},\ldots,\mathcal{H}_{B_n}$, *i.e.*, the test T has the following form:

$$T = \sum_i a_i T_i^{A_1}\otimes\cdots\otimes T_i^{A_n}\otimes T_i^{B_1}\otimes\cdots\otimes T_i^{B_n},$$

where $a_i \ge 0$ and the matrix $T_i^{A_k}$ ($T_i^{B_k}$) is a positive semi-definite matrix on the system $\mathcal{H}_{A_k}$ ($\mathcal{H}_{B_k}$), respectively.

$L(A_1,\ldots,A_n,B_1,\ldots,B_n)$: The test can be realized by two-way LOCC among $2n$ systems $\mathcal{H}_{A_1},\ldots,\mathcal{H}_{A_n}$, $\mathcal{H}_{B_1},\ldots,\mathcal{H}_{B_n}$.

$L(A_1,\ldots,A_n \to B_1,\ldots,B_n)$: The test can be realized by LOCC among $2n$ systems $\mathcal{H}_{A_1},\ldots,\mathcal{H}_{A_n},\mathcal{H}_{B_1},\ldots,\mathcal{H}_{B_n}$. Moreover, the classical communication among two groups $\mathcal{H}_{A_1},\ldots,\mathcal{H}_{A_n}$ and $\mathcal{H}_{B_1},\ldots,\mathcal{H}_{B_n}$ is restricted to one-way from the former to the later.

Based on the above conditions, we define the following quantity as the optimal second error probability:

$$\beta^C_{\alpha,n,G}(\le\epsilon\|\sigma) \stackrel{\rm def}{=} \min_{T\in T^n_{\alpha,\le\epsilon}} \left\{\beta(T,\sigma^{\otimes n}) \,\middle|\, \begin{array}{l} T \text{ is } G\text{-invariant,} \\ \text{and satisfies } C \end{array}\right\}.$$

As is easily checked, any LOCC operation is separable. Hence, the condition $L(A \leftrightarrows B)$ is stronger than the condition $S(A,B)$. Also, the condition $L(A_1,\ldots,A_n \to B_1,\ldots,B_n)$ is stronger than the condition $S(A_1,\ldots,A_n \to B_1,\ldots,B_n)$. The relation among these conditions can be illustrated as follows.

Next, we focus on the trivial relations of the optimal second error probability. If a group G_1 is greater than G_2, the inequality

$$\beta^C_{\alpha,n,G_1}(\le\epsilon\|\sigma) \ge \beta^C_{\alpha,n,G_2}(\le\epsilon\|\sigma) \tag{2}$$

holds. Moreover, if a condition C_1 is stronger than another condition C_2, the similar inequality

$$\beta^{C_1}_{\alpha,n,G}(\le\epsilon\|\sigma) \ge \beta^{C_2}_{\alpha,n,G}(\le\epsilon\|\sigma) \tag{3}$$

holds.

Similarly, we define $\beta^C_{\alpha,n,G}(\ge\epsilon\|\sigma)$ by replacing $\le\epsilon$ by $\ge\epsilon$ in RHS.

Indeed, if the condition is invariant for the action of G, it is very natural to restrict our test among G-invariant tests, as is indicated by the following lemma.

Lemma 1 *Assume that a set of test satisfying the condition C is invariant for the action of G, Then*

$$\beta^C_{\alpha,n,G}(\le \epsilon\|\sigma) = \min_{T\in\mathcal{T}^n_{\alpha,\le\epsilon}} \max_{g\in G} \beta(T,(f(g)\sigma f(g)^\dagger)^{\otimes n})$$
$$= \min_{T\in\mathcal{T}^n_{\alpha,\le\epsilon}} \int_G \beta(T,(f(g)\sigma f(g)^\dagger)^{\otimes n})\nu_G(dg),$$

where ν_G is the invariant measure and f denotes the action of G.

In the following, we sometimes abbreviate the invariant measure ν_G by ν. This lemma is a special version of quantum Hunt-Stein lemma [2, 3]. The condition $\emptyset$ is invariant for the actions $U(1), SU(d), SU(d)\times U(1), U(d^2-1)$. But, other conditions $S(A,B), L(A \leftrightarrows B), L(A \to B), S(A_1,\ldots,A_n,B_1,\ldots B_n), L(A_1,\ldots,A_n,B_1,\ldots B_n), L(A_1,\ldots A_n \to B_1,\ldots B_n)$ are invariant only for $SU(d)$. Hence, Lemma 1 cannot be applied to the pair of these conditions and the actions $U(1), SU(d), SU(d)\times U(1), U(d^2-1)$. The following lemma is useful in such a case.

Lemma 2 *Assume that the group G_1 includes another group G_2 which satisfies the condition of Lemma 1. If*

$$\beta^C_{\alpha,n,G_1}(\le\epsilon\|\sigma) = \beta^C_{\alpha,n,G_2}(\le\epsilon\|\sigma), \quad \forall\sigma$$

then

$$\beta^C_{\alpha,n,G_1}(\le\epsilon\|\sigma)$$
$$= \min_{T\in\mathcal{T}^n_{\alpha,<\epsilon}} \max_{g\in G_1} \beta(T,(f(g)\sigma f(g)^\dagger)^{\otimes n})$$
$$= \min_{T\in\mathcal{T}^n_{\alpha,<\epsilon}} \int_{G_1} \beta(T,(f(g)\sigma f(g)^\dagger)^{\otimes n})\nu_{G_1}(dg).$$

IV. TESTING FOR BINOMIAL DISTRIBUTIONS

In this paper, we use several knowledges about testing for binomial distributions for testing for a maximally entangled state. Hence, we review them here.

A. One-sample setting:

As a preliminary, we treat testing for the coin flipping probability p with a single trial. That is, we assume that the event 1 happens with the probability p and the event 0 happens with the probability $1-p$, and focus on the null hypothesis $p\in[0,\epsilon]$. In this case, our test can be described by a map $\tilde{T}$ from $\{0,1\}$ to $[0,1]$, which means that when the data k is observed, we accept the null hypothesis with the probability $\tilde{T}(k)$. Then, the minimum second error probability among level-α tests is given by

$$\beta^1_\alpha(\le\epsilon\|q) \stackrel{\rm def}{=} \min_{\tilde{T}} \left\{ q(\tilde{T}) \middle| \forall p\in[0,\epsilon], p(\tilde{T}) \ge 1-\alpha \right\}$$
$$p(\tilde{T}) \stackrel{\rm def}{=} (1-p)\tilde{T}(0) + p\tilde{T}(1)$$

When we define the test $\tilde{T}^1_{\epsilon,\alpha}$ by

$$\tilde{T}^1_{\epsilon,\alpha}(0) = \begin{cases} \frac{1-\alpha}{1-\epsilon} & \text{if } \epsilon\le\alpha \\ 1 & \text{if } \epsilon>\alpha \end{cases}, \quad \tilde{T}^1_{\epsilon,\alpha}(1) = \begin{cases} 0 & \text{if } \epsilon\le\alpha \\ \frac{\epsilon-\alpha}{\epsilon} & \text{if } \epsilon>\alpha, \end{cases}$$

the test $\tilde{T}^1_{\epsilon,\alpha}$ satisfies

$$(1-\epsilon)\tilde{T}^1_{\epsilon,\alpha}(0) + \epsilon\tilde{T}^1_{\epsilon,\alpha}(1) = 1-\alpha. \tag{4}$$

Moreover, if $p\le\epsilon$,

$$(1-p)\tilde{T}^1_{\epsilon,\alpha}(0) + p\tilde{T}^1_{\epsilon,\alpha}(1) \ge 1-\alpha.$$

Hence the test $\tilde{T}^1_{\epsilon,\alpha}$ is level-α. Furthermore, we can easily check that the minimum of $q(\tilde{T})$ with the condition (4) for $\tilde{T}$ can be attained by $\tilde{T}=\tilde{T}^1_{\epsilon,\alpha}$ if $q>\epsilon$. Hence,

$$\beta^1_\alpha(\le\epsilon\|q) = q(\tilde{T}^1_{\epsilon,\alpha}) = \begin{cases} \frac{(1-\alpha)(1-q)}{1-\epsilon} & \text{if } \epsilon\le\alpha \\ 1-\frac{\alpha q}{\epsilon} & \text{if } \epsilon>\alpha. \end{cases} \tag{5}$$

B. n-sample setting:

In the n-trial case, the data $k=0,1,\ldots,n$ obeys the distribution $P^n_p(k) \stackrel{\rm def}{=} \binom{n}{k}(1-p)^{n-k}p^k$ with the unknown parameter p. Hence, we discuss the hypothesis testing with the null hypothesis $\mathcal{P}^n_{\le\epsilon} \stackrel{\rm def}{=} \{P^n_p(k)|p\le\epsilon\}$ and the alternative hypothesis $(\mathcal{P}^n_{\le\epsilon})^c$. In this case, our test $\tilde{T}$ can be described by a function from the data set $\{0,1,\ldots,n\}$ to interval $[0,1]$. In this case, when the data k is observed, we accept the null hypothesis $\mathcal{P}^n_{\le\epsilon}$ with the probability $T(k)$. Then, the minimum second error probability among level-α tests is given by

$$\beta^n_\alpha(\le\epsilon\|q) \stackrel{\rm def}{=} \min_{\tilde{T}} \left\{ P^n_q(\tilde{T}) \middle| \forall p\in[0,\epsilon], 1-P^n_p(\tilde{T}) \le \alpha \right\}$$
$$P^n_p(\tilde{T}) \stackrel{\rm def}{=} \sum_{k=0}^n P^n_p(k)\tilde{T}(k).$$

We define the test $\tilde{T}^n_{\epsilon,\alpha}$ as follows.

$$\tilde{T}^n_{\epsilon,\alpha}(k) = \begin{cases} 1 & k < l^n_{\epsilon,\alpha} \\ \gamma^n_{\epsilon,\alpha} & k = l^n_{\epsilon,\alpha} \\ 0 & k > l^n_{\epsilon,\alpha}, \end{cases}$$

where the integer $l^n_{\epsilon,\alpha}$ and the real number $\gamma^n_{\epsilon,\alpha}>0$, are defined by

$$\sum_{k=0}^{l^n_{\epsilon,\alpha}-1} P^n_\epsilon(k) < 1-\alpha \le \sum_{k=0}^{l^n_{\epsilon,\alpha}} P^n_\epsilon(k)$$
$$\gamma^n_{\epsilon,\alpha}P^n_\epsilon(l^n_{\epsilon,\alpha}) = 1-\alpha - \sum_{k=0}^{l^n_{\epsilon,\alpha}-1} P^n_\epsilon(k).$$

Theorem 1 *The test $\tilde{T}^n_{\epsilon,\alpha}$ is level-α UMP test with the null hypothesis $\mathcal{P}^n_{\le\epsilon}$. Hence,*

$$\beta^n_\alpha(\le\epsilon\|q) = P^n_q(\tilde{T}_{\epsilon,\alpha}) = \sum_{k=0}^{l^n_{\epsilon,\alpha}-1} P^n_q(k) + \gamma^n_{\epsilon,\alpha}P^n_q(l^n_{\epsilon,\alpha}).$$

C. Asymptotic setting

In asymptotic theory, There are two settings at least. One is the large deviation setting, in which the parameter is fixed, hence we focus on the exponential component of the error probability. The other is the small deviation setting, in which the parameter is close to a given fixed point in proportion to the number of samples such that the error probability converges to a fixed number. That is, the parameter is fixed in the former, while the error probability is fixed in the later.

1. Small deviation theory

It is useful to treat the neiborhood around $p = 0$ as the small deviation theory of this problem for the asymptotic discussion of testing for an maximally entangled state. Hence, we focus on the case that $p = \frac{t}{n}$: Since the probability $P^n_{t/n}(k) = \binom{n}{k}(1-\frac{t}{n})^{n-k}\left(\frac{t}{n}\right)^k$ convergences to the Poisson distribution $P_t(k) \stackrel{\rm def}{=} e^{-t}\frac{t^k}{k!}$. Hence, our testing problem with the null hypothesis $\mathcal{P}_{\frac{\delta}{n}}$ and the alternative hypothesis $\frac{t'}{n}$. is asymptotically equivalent with the testing of Poisson distribution $P_t(k)$ with the null hypothesis $t \in [0, \delta]$ and the alternative hypothesis t'. That is, by defining

$$\beta_\alpha(\le \delta \| t') \stackrel{\rm def}{=} \min_{\tilde{T}} \left\{ P_{t'}(\tilde{T}) \middle| \forall t \in [0,\delta], 1 - P_t(\tilde{T}) \le \alpha \right\}$$
$$P_t(\tilde{T}) \stackrel{\rm def}{=} \sum_{k=0}^{\infty} P_t(k)\tilde{T}(k),$$

the following theorem holds.

Theorem 2

$$\lim \beta^n_\alpha \left(\le \frac{\delta}{n} \middle\| \frac{t'}{n} \right) = \beta_\alpha(\le \delta \| t').$$

Similarly to the test $\tilde{T}^n_{\epsilon,\alpha}$, we define the test $\tilde{T}_{\delta,\alpha}$ as

$$\tilde{T}_{\delta,\alpha}(k) = \begin{cases} 1 & k < l_{\delta,\alpha} \\ \gamma_{\delta,\alpha} & k = l_{\delta,\alpha} \\ 0 & k > l_{\delta,\alpha}, \end{cases}$$

where the integer $l_{\delta,\alpha}$ and the real number $\gamma_{\delta,\alpha} > 0$, are defined by

$$\sum_{k=0}^{l_{\delta,\alpha}-1} P_\delta(k) < 1-\alpha \le \sum_{k=0}^{l_{\delta,\alpha}} P_\delta(k)$$
$$\gamma_{\delta,\alpha} P_\delta(l_{\delta,\alpha}) = 1 - \alpha - \sum_{k=0}^{l^n_{\delta,\alpha}-1} P_\delta(k).$$

Similarly to Theorem 1, the following theorem holds.

Theorem 3 *The test $\tilde{T}_{\delta,\alpha}$ is level-α UMP test with the null hypothesis $\mathcal{P}_{\le\delta} \stackrel{\rm def}{=} \{P_t | t \le \delta\}$. Hence,*

$$\beta^n_\alpha(\le \delta \| t') = \sum_{k=0}^{l_{\delta,\alpha}-1} P_{t'}(k) + \gamma_{\delta,\alpha} P_{t'}(l_{\delta,\alpha}).$$

2. Large deviation theory

Next, we proceed to the large deviation theory. Using the knowledge of mathematical statistics, we can calculate the exponents of the 2nd error probabilities $\beta^n_\alpha(\epsilon\|p)$ and $\beta^n_\alpha(\epsilon\|p)'$ for any $\alpha > 0$ as

$$\lim \frac{-1}{n} \log \beta^n_\alpha(\le \epsilon \| p) = d(\epsilon\|p), \text{ if } \epsilon < p$$
$$\lim \frac{-1}{n} \log \beta^n_\alpha(\ge \epsilon \| p) = d(\epsilon\|p), \text{ if } \epsilon > p,$$

where the binary relative entropy $d(\epsilon\|p)$ is defined as

$$d(\epsilon\|p) \stackrel{\rm def}{=} \epsilon \log \frac{\epsilon}{p} + (1-\epsilon)\log\frac{1-\epsilon}{1-p}.$$

In the case of $\alpha = 0$, we have

$$\frac{-1}{n}\log\beta^n_0(\epsilon\|p) = \begin{cases} -\log(1-p) & \text{if } \epsilon = 0 \\ 0 & \text{if } \epsilon \neq 0. \end{cases}$$

V. GLOBAL TESTS

First, we treat the hypotheses testing with a given group invariance condition with no locality restriction.

A. One-sample setting:

When only one sample is prepared, the test $|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|$ is a level-0 test for the null hypothesis $\mathcal{S}_0$. If we perform the two-valued measurement $\{|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|, I - |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|\}$, the data obeys the distribution $\{1-p, p\}$, where

$$p \stackrel{\rm def}{=} 1 - \langle\phi^0_{A,B}|\sigma|\phi^0_{A,B}\rangle.$$

Hence, applying the discussion in subsection IV A, the test $T^1_\alpha(|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|, \epsilon)$ is a level-α test for the null hypothesis $\mathcal{S}_{\le\epsilon}$, where the operator $T^1_\alpha(T,\epsilon)$ is defined by

$$T^1_\alpha(T,\epsilon) \stackrel{\rm def}{=} \begin{cases} \frac{1-\alpha}{1-\epsilon}T & \text{if } \epsilon \le \alpha \\ T + \frac{\epsilon-\alpha}{\epsilon}(I-T) & \text{if } \epsilon > \alpha. \end{cases}$$

B. n-sample setting:

In the n-sample setting, we construct a test for the null hypothesis $\mathcal{S}_{\le\epsilon}$ as follows. First, we perform the two-valued measurement $\{|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|, I - |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|\}$ for

respective n systems. Then, if the number of counting $I - |\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|$ is described by k, the data k obeys the binomial distribution $P_p^n(k)$. In this case, our problem can be reduced to the hypothesis testing with the null hypothesis $\mathcal{P}_{\le\epsilon}^n$, which has been discussed in subsection IV B.

For given α and ϵ, the test based on this measurement and the classical test $\tilde{T}_{\epsilon,\alpha}^n$ is described by the operator $T_{\epsilon,\alpha}^n \stackrel{\rm def}{=} T_\alpha^n(|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|, \epsilon)$, where $T_\alpha^n(T,\epsilon)$ is defined by

$$T_\alpha^n(T,\epsilon) \stackrel{\rm def}{=} \sum_{k=0}^{l_\alpha^n(\epsilon)-1} P_k^n(T, I-T) + \gamma_\alpha^n(\epsilon) P_{l_\alpha^n(\epsilon)}^n(T, I-T)$$

$$P_{n,k}(T,S) \stackrel{\rm def}{=} \underbrace{S\otimes\cdots\otimes S}_{k}\otimes\underbrace{T\otimes\cdots\otimes T}_{n-k} + \cdots + \underbrace{T\otimes\cdots\otimes T}_{n-k}\otimes\underbrace{S\otimes\cdots\otimes S}_{k}.$$

Note that the above sum contains all tensor products of k times of S and $n-k$ times of T.

Since the operators $|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|$ and $I - |\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|$ are $U(d^2-1)$-invariant, the test $T_{\epsilon,\alpha}^n$ is level-α $U(d^2-1)$-invariant test with the hypothesis $\mathcal{S}_{\le\epsilon}$. Hence,

$$\beta^{\emptyset}_{\alpha,n,U(d^2-1)}(\le\epsilon\|\sigma) \le \beta_\alpha^n(\le\epsilon\|p). \tag{6}$$

$$\beta^{\emptyset}_{\alpha,n,U(1)}(\le\epsilon\|\sigma) = \beta_\alpha^n(\le\epsilon\|p). \tag{7}$$

Since $U(1) \subset SU(d)\times U(1) \subset U(d^2-1)$, the relations (6) and (7) yield the following theorem.

Theorem 4 *The equation*

$$\beta^{\emptyset}_{\alpha,n,G}(\le\epsilon\|\sigma) = \beta_\alpha^n(\le\epsilon\|p) \tag{8}$$

holds for $G = U(1), SU(d)\times U(1), U(d^2-1)$.

Therefore, The test $T_{\epsilon,\alpha}^n$ is the UMP G-invariant test, for $G = U(1), SU(d)\times U(1)$ or $U(d^2-1)$. Moreover, we can derive the same results for the hypothesis $\mathcal{S}_{\ge\epsilon}$.

C. Asymptotic setting

Next, we proceed to the asymptotic setting. In the small deviation theory, we treat the hypothesis testing with the null hypothesis $\mathcal{S}_{\le\delta/n}$. in this setting, Theorem 2 and Theorem 4 guarantee that the limit of the optimal second error probability of the alternative hypothesis σ_n is given by $\beta_\alpha(\delta\|t')$ if $\langle\phi_{A,B}^0|\sigma_n|\phi_{A,B}^0\rangle = 1 - \frac{t'}{n}$. That is,

$$\lim \beta_{\alpha,G}^n\left(\le\frac{\delta}{n}\middle\|\,\sigma_n\right) = \beta_\alpha(\le\delta\|t') \tag{9}$$

for $G = U(1), SU(d)\times U(1), U(d^2-1)$.

In the large deviation setting, we can obtain the same results as subsection IV C, *i.e.*,

$$\lim\frac{-1}{n}\log\beta_{\alpha,G}^n(\le\epsilon\|\sigma) = \begin{cases} d(\epsilon\|p) & \text{if } \alpha > 0 \\ -\log(1-p) & \text{if } \alpha = 0, \epsilon = 0 \\ 0 & \text{if } \alpha = 0, \epsilon > 0 \end{cases} \tag{10}$$

if $\epsilon < p = 1 - \langle\phi_{A,B}^0|\sigma|\phi_{A,B}^0\rangle$. Moreover, we can derive similar results with the null hypothesis $\mathcal{S}_{\ge\epsilon}$.

VI. A-B LOCALITY

In this section, we treat optimization problems with several conditions regarding the locality between A and B.

A. One-sample setting

First, we focus on the simplest case, *i.e.*, the case of $\epsilon = 0$ and $\alpha = 0$. For this purpose, we focus on a POVM with the following form on $\mathcal{H}_A$

$$M = \{p_i|u_i\rangle\langle u_i|\}_i, \quad \|u_i\| = 1, \quad 0 \le p_i \le 1,$$

where such a POVM is called *rank-one*. Based on a rank-one POVM M, a suitable test $T(M)$

$$T(M) \stackrel{\rm def}{=} \sum_i p_i |u_i\otimes\overline{u_i}\rangle\langle u_i\otimes\overline{u_i}|. \tag{11}$$

can be realized by the following one-way LOCC protocol. From the definition, of course, we can easily check that $T(M)$ satisfies the condition of test, *i.e.*,

$$0 \le T(M) \le I. \tag{12}$$

One-way LOCC protocol of $T(M)$:
1) Alice performs the measurement $\{p_i|u_i\rangle\langle u_i|\}_i$, and sends her data i to Bob.
2) Bob performs the two-valued measurement $\{|\overline{u_i}\rangle\langle\overline{u_i}|, I - |\overline{u_i}\rangle\langle\overline{u_i}|\}$, where $\overline{u_i}$ is the complex conjugate of u_i concerning the standard basis $|0\rangle_B, |1\rangle_B, ..., |d-1\rangle_B$.
3) If Bob observes the event corresponding to $|\overline{u_i}\rangle\langle\overline{u_i}|$, the hypothesis $|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|$ is accepted. Otherwise, it is rejected.

This test satisfies

$$\langle\phi_{A,B}^0|T(M)|\phi_{A,B}^0\rangle = 1, \tag{13}$$

$$\mathrm{Tr}\, T(M) = \sum_i p_i \,\mathrm{Tr}\,|u_i\otimes\overline{u_i}\rangle\langle u_i\otimes\overline{u_i}| = \sum_i p_i \,\mathrm{Tr}\,|u_i\rangle\langle u_i| = d. \tag{14}$$

Hence, it is a level-0 test with the null hypothesis $|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|$. In particular, in the one-way LOCC setting, our test can be restricted to this kind of tests as the following sense.

Lemma 3 *Let T be a one-way LOCC $(A \to B)$ level-0 test with the null hypothesis $|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|$. Then, there exists a POVM with the form $M = \{p_i|u_i\rangle\langle u_i|\}_i$ such that*

$$T \geq T(M), \tag{15}$$

i.e., the test $T(M)$ is better than the test T.

Moreover, concerning the separable condition, the following lemma holds. Hence, Corollary 1 indicates that it seems natural to restrict our test to the test with the form (11) even if we adopt the separable condition.

Lemma 4 *Assume that a separable test T satisfies*

$$\langle\phi^0_{A,B}|T|\phi^0_{A,B}\rangle = 1. \tag{16}$$

When we describe the test T as

$$T = d\sum_i p_i|u_i\otimes u'_i\rangle\langle u_i\otimes u'_i| + \sum_j q_j|v_i\otimes v'_i\rangle\langle v_i\otimes v'_i|, \tag{17}$$

such that $\langle\phi^0_{A,B}|u_i\otimes u'_i\rangle = \frac{1}{\sqrt{d}}$ and $\langle\phi^0_{A,B}|v_i\otimes v'_i\rangle = 0$, we obtain

$$\sum_i p_i u_i\otimes u'_i = \frac{1}{\sqrt{d}}\phi^0_{A,B}.$$

Note that we can easily obtain the same statement if we replace the summation $\sum_i$ by the integral $\int$ at (17). Since any separable test T has the form (17), the following corollary holds concerning the completely mixed state $\frac{I}{d^2}$.

Corollary 1 *If a separable test T satisfies the conditions*

$$\langle\phi^0_{A,B}|T|\phi^0_{A,B}\rangle = 1$$
$$\mathrm{Tr}\, T\frac{I}{d^2} = d = \min_{T'\in S(A,B)}\left\{\mathrm{Tr}\, T'\frac{I}{d^2}\middle|\ \langle\phi^0_{A,B}|T'|\phi^0_{A,B}\rangle = 1\right\},$$

then the test T has a form (11).

Next, we focus on the covariant POVM M^1_{cov}:

$$M^1_{cov}(d\varphi) \stackrel{\mathrm{def}}{=} d|\varphi\rangle\langle\varphi|\nu(d\varphi),$$

where $\nu(d\varphi)$ is the invariant measure in the set of pure states with the full measure is 1. Then, the test $T^{1,A\to B}_{inv} \stackrel{\mathrm{def}}{=} T(M^1_{cov})$ has the following form

$$\begin{aligned} T^{1,A\to B}_{inv} &= \int d|\varphi\otimes\overline{\varphi}\rangle\langle\varphi\otimes\overline{\varphi}|\nu(d\varphi) \\ &= |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}| + \frac{1}{d+1}(I - |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|). \end{aligned} \tag{18}$$

Note that the POVM M^1_{cov} can be realized as follows:

Realization of M^1_{cov}:

1) Randomly, we choose $g \in SU(d)$ with the invariant measure.

2) Perform POVM $\{g|i\rangle_A\ {}_A\langle i|g^\dagger\}_i$. Then, the realized POVM is M^1_{cov}.

Since the equation (18) guarantees the $U(d^2-1)$-invariance of the test $T^{1,A-B}_{inv}$, we obtain

$$\mathrm{Tr}\, T^{1,A\to B}_{inv}\sigma = 1 - p + \frac{p}{d+1} = 1 - \frac{dp}{d+1},$$

which implies

$$\beta^{L(A\to B)}_{0,1,U(d^2-1)}(0\|\sigma) \leq 1 - \frac{dp}{d+1}.$$

Next, we apply the discussion in subsection IV A to the probability distribution $\{\frac{dp}{d+1}, 1-\frac{dp}{d+1}\}$. Then, the test $T^{1,A-B}_{\epsilon,\alpha} \stackrel{\mathrm{def}}{=} T^1_\alpha(T^{1,A-B}_{inv}, \frac{d\epsilon}{d+1})$ is a level-α $U(d^2-1)$-invariant test. Since the test $T^{1,A-B}_{\epsilon,\alpha}$ can be performed by randomized operation with $T^{1,A-B}_{inv}$ and $I - T^{1,A-B}_{inv}$, we obtain

$$\begin{aligned} &\beta^{L(A\to B)}_{\alpha,1,U(d^2-1)}(\leq\epsilon\|\sigma) \leq \mathrm{Tr}\, T^{1,A-B}_{\epsilon,\alpha}\sigma \\ &= \begin{cases} \frac{(1-\alpha)(1-\frac{d}{d+1}p)}{(1-\frac{d}{d+1}\epsilon)} & \text{if } \frac{d}{d+1}\epsilon \leq \alpha \\ 1 - \frac{\alpha p}{\epsilon} & \text{if } \frac{d}{d+1}\epsilon > \alpha, \end{cases} \end{aligned} \tag{19}$$

On the other hand, concerning $SU(d)$-invariance and separable tests, the equation

$$\beta^{S(A,B)}_{\alpha,1,SU(d)}(\leq\epsilon\|\sigma) = \mathrm{Tr}\, T^{1,A-B}_{\epsilon,\alpha}\sigma \tag{20}$$

holds. The equation in the case of $\alpha = 0, \epsilon = 0$ is obtained by Tsuda *et al.*[1]. A similar result with the PPT condition is appeared in Virmani and Plenio [21].

Since $U(d^2-1)$ is a larger group action than $SU(d)$ and the condition $L(A \to B)$ is stricter than the condition $S(A,B)$, the trivial inequalities

$$\begin{aligned} &\beta^{S(A,B)}_{\alpha,1,SU(d)}(\leq\epsilon\|\sigma) \leq \beta^{S(A,B)}_{\alpha,1,U(d^2-1)}(\leq\epsilon\|\sigma) \\ \leq &\beta^{L(A\to B)}_{\alpha,1,U(d^2-1)}(\leq\epsilon\|\sigma) \end{aligned}$$

hold. Therefore, relations (19) and (20) yield

$$\beta^C_{\alpha,1,G}(\leq\epsilon\|\sigma) = \begin{cases} \frac{(1-\alpha)(1-\frac{d}{d+1}p)}{(1-\frac{d}{d+1}\epsilon)} & \text{if } \frac{d}{d+1}\epsilon \leq \alpha \\ 1 - \frac{\alpha p}{\epsilon} & \text{if } \frac{d}{d+1}\epsilon > \alpha, \end{cases} \tag{21}$$

for $G = SU(d), SU(d)\times U(1), U(d^2-1)$, and $C = L(A\to B), L(A \leftrightarrows B), S(A,B)$. That is, the test $T^{1,A-B}_{\epsilon,\alpha}$ is the UMP G-invariant C test with level α for the null hypothesis $\mathcal{S}_{\leq\epsilon}$. Furthermore, similar results for the null hypothesis $\mathcal{S}_{\geq\epsilon}$ can be also obtained.

B. Two-sample case

In this section, we construct a $SU(d)\times U(1)$-invariant test which is realized by LOCC between A and B, and

which attains the asymptotically optimal bound (9). For this purpose, we focus on the covariant POVM M_{cov}^2:

$$\begin{aligned} & M_{cov}^2(\,dg_1\,dg_2) \\ \stackrel{\rm def}{=} & d^2(g_1\otimes g_2)|u\rangle\langle u|(g_1\otimes g_2)^*\nu(\,dg_1)\nu(\,dg_2), \end{aligned}$$

where the vector u is maximally entangled and ν is the invariant measure on $SU(d)$. Then, the operator $T_{inv}^{2,A\to B}\stackrel{\rm def}{=} T(M_{cov}^2)$ has the form:

$$\begin{aligned} & T_{inv}^{2,A\to B} \\ =& |\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|\otimes|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0| \\ & + \frac{1}{d^2-1}(I-|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|)\otimes(I-|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|). \end{aligned} \tag{22}$$

This equation implies that the testing $T(M_{cov}^2)$ does not depend on the choice of the maximally entangled state u. It also guarantees the $U(d^2-1)$-invariance of the test $T_{inv}^{2,A\to B}$. We also obtain the equation

$$\mathrm{Tr}\, T_{inv}^{2,A\to B}\sigma^{\otimes 2} = (1-p)^2+\frac{p^2}{d^2-1} = 1-2p+\frac{d^2p^2}{d^2-1}. \tag{23}$$

Since the test $T_{inv}^{2,A\to B}$ is a level-0 test with the null hypothesis $\mathcal{S}_0$, the inequality

$$\beta_{0,2,U(d^2-1)}^{L(A\to B)}(0\|\sigma)\le 1-2p+\frac{d^2p^2}{d^2-1}$$

holds. Next, we apply the discussion of subsection IV A. Then, the test $T_{\epsilon,\alpha}^{2,A-B}\stackrel{\rm def}{=} T_\alpha^1(T_{inv}^{2,A\to B},2\epsilon-\frac{d^2\epsilon^2}{d^2+1})$ is a level-α $U(d^2-1)$-invariant test. Since the test $T_{\epsilon,\alpha}^{2,A-B}$ can be performed by randomized operation with $T_{inv}^{2,A\to B}$ and $I-T_{inv}^{2,A\to B}$, we obtain

$$\begin{aligned} & \beta_{\alpha,2,U(d^2-1)}^{L(A\to B)}(\le\epsilon\|\sigma)\le \mathrm{Tr}\, T_{\epsilon,\alpha}^{2,A-B}\sigma^{\otimes 2} \\ =& \begin{cases} \frac{(1-\alpha)(1-2p+\frac{d^2p^2}{d^2+1})}{1-2\epsilon+\frac{d^2\epsilon^2}{d^2+1}} & \text{if } 2\epsilon-\frac{d^2\epsilon^2}{d^2+1}\le\alpha \\ 1-\frac{\alpha(2p+\frac{d^2p^2}{d^2-1})}{2\epsilon-\frac{d^2\epsilon^2}{d^2-1}} & \text{if } 2\epsilon-\frac{d^2\epsilon^2}{d^2+1}>\alpha. \end{cases} \end{aligned}$$

Furthermore, as a generalization of (23), we obtain the following lemma, which is more useful in the asymptotic setting from an applied viewpoint.

Lemma 5 *Let $M=\{p_i|u_i\rangle\langle u_i|\}(\||u_i\|\|=1)$ be a POVM on A's two-sample space $\mathcal{H}_A^{\otimes 2}$. If every state $|u_i\rangle$ is a maximally entangled state on $\mathcal{H}_A^{\otimes 2}$, the test $T(M)$ satisfies*

$$\begin{aligned} \langle\phi_{AB}^0|\sigma|\phi_{AB}^0\rangle^2 \le & \mathrm{Tr}\,\sigma^{\otimes 2}T(M) \\ \le & \langle\phi_{AB}^0|\sigma|\phi_{AB}^0\rangle^2+(1-\langle\phi_{AB}^0|\sigma|\phi_{AB}^0\rangle)^2. \end{aligned}$$

Indeed, it is difficult to realize the covariant POVM M_{cov}^2. The Bell measurement $M_{Bell}^2\stackrel{\rm def}{=}\{|\phi_{1,2}^{n,m}\rangle\langle\phi_{1,2}^{n,m}|\}_{(n,m)=(0,0)}^{(d-1,d-1)}$ can be constructed more easily, where $\phi_{1,2}^{n,m}$ is defined by

$$\begin{aligned} \phi_{1,2}^{0,0} &\stackrel{\rm def}{=} \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_{A,1}|j\rangle_{A,2} \\ \phi_{1,2}^{n,m} &\stackrel{\rm def}{=} ((X^nZ^m)\otimes I)\,\phi_{1,2}^{0,0} \\ X &\stackrel{\rm def}{=} \sum_{j=1}^{d-1}|j\rangle\langle j-1|+|0\rangle\langle d-1| \\ Z &\stackrel{\rm def}{=} \sum_{j=0}^{d-1}e^{2\pi ji/d}|j\rangle\langle j|. \end{aligned}$$

As will be mentioned in subsection VI D, the test $T(M_{Bell}^2)$ can be used as the alternative test of $T_{inv}^{2,A\to B}$ in an asymptotic sense.

C. n-sample setting

Next, we construct a $U(d^2-1)$-invariant test when $2n$ samples of the unknown state σ are prepared. It follows from a discussion similar to subsection V B that the test $T_{\epsilon,\alpha}'^{2n}\stackrel{\rm def}{=} T_\alpha^{2n}(T_{inv}^{2,A\to B},2\epsilon-\frac{d^2\epsilon^2}{d^2-1})$ is level-α for given α and ϵ. The $U(d^2-1)$-invariance of the test $T_{inv}^{2,A\to B}$ implies the $U(d^2-1)$-invariance of the test $T_{\epsilon,\alpha}'^{2n}$. Since the test $T_{\epsilon,\alpha}'^{2n}$ can be realized by one-way LOCC $A\to B$, the inequality

$$\begin{aligned} \beta_{\alpha,2n,U(d^2-1)}^{L(A\to B)}(\le\epsilon\|\sigma) \le & \mathrm{Tr}\, T_{\epsilon,\alpha}'^{2n}\sigma^{\otimes 2n} \\ = & \beta_\alpha^n\left(\le 2\epsilon-\frac{d^2\epsilon^2}{d^2-1}\,\middle\|\, 2p-\frac{d^2p^2}{d^2-1}\right) \end{aligned} \tag{24}$$

holds. In addition, we can derive a similar bound for the hypothesis $\mathcal{S}_{\ge\epsilon}$.

Concerning the case of $\epsilon=0$, we have another bound as follows. For this purpose, we focus on the test $T_{inv}^{1,A\to B}$ in the case when $\mathcal{H}_A=\mathcal{H}_A^{\otimes n}$ and $\mathcal{H}_B=\mathcal{H}_B^{\otimes n}$. Denoting this test by $T_{inv}^{1,A^{\otimes n}\to B^{\otimes n}}$, we have

$$\begin{aligned} T_{inv}^{1,A^{\otimes n}\to B^{\otimes n}} =& |\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|^{\otimes n} \\ & + \frac{1}{d^n+1}(I-|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|^{\otimes n}) \\ \mathrm{Tr}\, T_{inv}^{1,A^{\otimes n}\to B^{\otimes n}}\sigma^{\otimes n} =& \frac{d^n(1-p)^n+1}{d^n+1} \end{aligned}$$

because $\mathrm{Tr}\,|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|^{\otimes n}\sigma^{\otimes n}=(1-p)^n$. Since this test is $U(d^2-1)$-invariant, we obtain

$$\beta_{\alpha,n,U(d^2-1)}^{L(A\to B)}(0\|\sigma)\le\frac{d^n(1-p)^n+1}{d^n+1}. \tag{25}$$

D. Asymptotic setting

We proceed to asymptotic setting. First, we show that even if our test satisfies the A-B LOCC condition, the bound (8) can be attained in the asymptotic small deviation setting. Indeed, since $P^n_{2\frac{t}{2n}-\frac{d^2}{d^2-1}(\frac{t}{2n})^2}(k) \to P_t(k)$, the equation

$$\lim \beta^n_\alpha \left(\le 2\frac{\delta}{2n} - \frac{d^2}{d^2-1}\left(\frac{\delta}{2n}\right)^2 \middle\| 2\frac{t'}{2n} - \frac{d^2}{d^2-1}\left(\frac{t'}{2n}\right)^2 \right) = \beta_\alpha(\le \delta \| t')$$

can be proven similarly to Theorem 2. Hence, from (2) and (3), we have

$$\lim \beta^C_{\alpha,2n,G}(\le \frac{\delta}{n}\|\sigma_n) = \beta_\alpha(\le \delta\|t')$$

for $G = U(1), SU(d) \times U(1), U(d^2-1)$, $C = \emptyset, L(A \to B), L(A \leftrightarrows B), S(A,B)$. However, it is difficult to realized the covariant POVM M^2_{cov} on $\mathcal{H}_A^{\otimes 2}$. Even if the test $T'^{2n}_{\epsilon,\alpha}$ is replaced by $T'^{2n}_{\epsilon,\alpha,Bell} \stackrel{\rm def}{=} T^n_\alpha(T(M^2_{Bell}), 2\epsilon - \frac{d^2\epsilon^2}{d^2-1})$, the bound $\beta_\alpha(\le \delta\|t')$ can be attained in the following asymptotic sense. The test $T'^{2n}_{\frac{\delta}{2n},\alpha,Bell}$ may be not level-α with the null hypothesis $\mathcal{S}_{\le \delta/2n}$, but is asymptotically level-α, *i.e.*,

$$\mathrm{Tr}\, T'^{2n}_{\frac{\delta}{2n},\alpha,Bell}\sigma_{2n}^{\otimes 2n} \to 1-\delta \tag{26}$$

if $\langle \phi^0_{A,B}|\sigma_n|\phi^0_{A,B}\rangle = 1 - \frac{\delta}{n}$. Moreover, if $\langle \phi^0_{A,B}|\sigma_n|\phi^0_{A,B}\rangle = 1 - \frac{t'}{n}$ and $t' > \delta$, the relation

$$\mathrm{Tr}\, T'^{n}_{\frac{\delta}{2n},\alpha,Bell}\sigma_n^{\otimes n} \to \beta_\alpha(\le \delta\|t') \tag{27}$$

holds. These relations (26) and (27) follow from Lemma 5. Hence, there is no advantage of use of entanglement between $\mathcal{H}_A$ and $\mathcal{H}_B$ for this testing in the asymptotic small deviation setting. Similar results for the null hypothesis $\mathcal{S}_{\ge \delta/n}$ can be obtained.

Next, we proceed to the large deviation setting. The inequality (25) yields

$$\lim \frac{-1}{n} \log \beta^{L(A\to B)}_{\alpha,n,U(d^2-1)}(0\|\sigma) \ge \begin{cases} -\log(1-p) & \text{if } 1-p \ge \frac{1}{d} \\ \log d & \text{if } 1-p < \frac{1}{d} \end{cases} \tag{28}$$

Hence, the relations (3) and (10) guarantee that if $1-p \ge \frac{1}{d}$,

$$\lim \frac{-1}{n} \log \beta^{L(A\to B)}_{\alpha,n,U(d^2-1)}(0\|\sigma) = -\log(1-p),$$

for $G = U(1), SU(d) \times U(1), U(d^2-1)$, $C = \emptyset, L(A \to B), L(A \leftrightarrows B), S(A,B)$. Hence, we can conclude that if $1-p \ge \frac{1}{d}$, there is no advantage of use of entanglement between $\mathcal{H}_A$ and $\mathcal{H}_B$ for this testing even in this kind of the asymptotic large deviation setting.

VII. A-B LOCALITY AND SAMPLE LOCALITY

In this section, we discuss the locality among $A_1, B_1, \ldots, A_n, B_n$. Since the case $n = 1$ of this setting is the same as that of the setting section VI. Hence, we treat the case $n = 2$, at first.

A. Two-sample setting

We construct a level-0 $SU(d)$-invariant test for the null hypothesis $\mathcal{S}_0 = \{|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|\}$ as follows. For this purpose, we define a POVM $M^{1\to 2}_{cov}$ on Alice's space $\mathcal{H}_A^{\otimes 2}$, which can be realized by one-way LOCC $A_1 \to A_2$ from the first system $\mathcal{H}_{A_1}$ to the second system $\mathcal{H}_{A_2}$.

Construction of $M^{1\to 2}_{cov}$:

1) Alice performs the covariant POVM M^1_{cov} on the first system $\mathcal{H}_{A_1}$, and obtain the data corresponding to the state $|\varphi\rangle\langle\varphi|$.

2) We choose the Projection-valued measure $\{|u^i(\varphi)\rangle\langle u^i(\varphi)|\}_i$ satisfying that

$$\langle u^i(\varphi)|u^j(\varphi)\rangle = 0, \quad \langle u^i(\varphi)|\varphi\rangle = \frac{1}{\sqrt{d}}. \tag{29}$$

3) Alice randomly chooses $g \in U(d-1)$ which acts on the space orthogonal to φ, and performs the Projection-valued measure $\{|gu^i(\varphi)\rangle\langle gu^i(\varphi)|\}_i$ on the second system $\mathcal{H}_{A_2}$.

Since Bob's measurement of the test $T(M^{1\to 2}_{cov})$ can be also realized by one-way LOCC on Bob's space, this test is a $L(A_1, A_2 \to B_1, B_2)$ test. Its POVM is given by

$$M^{1\to 2}_{cov}(\,dg) = d^2(g\otimes g)|u_1\otimes u_2\rangle\langle u_1\otimes u_2|(g\otimes g)^\dagger \nu(\,dg),$$

where we choose u_1 and u_2 satisfying $|\langle u_1|u_2\rangle|^2 = \frac{1}{d}$. Thus, the $SU(d)$-covariance of $M^{1\to 2}_{cov}$ guarantees the $SU(d)$-invariance of the test $T^{A_1\to A_2\to B^{\otimes 2}}_{inv} \stackrel{\rm def}{=} T(M^{1\to 2}_{cov})$. the test $T^{A_1\to A_2\to B^{\otimes 2}}_{inv}$ is $U(1)$-invariant. Hence, the inequality

$$\beta^{L(A_1,A_2\to B_1,B_2)}_{0,2,SU(d)\times U(1)}(0\|\sigma) \le \mathrm{Tr}\, T^{A_1\to A_2\to B^{\otimes 2}}_{inv}\sigma^{\otimes 2}$$

holds. On the other hand, the equation

$$\beta^{L(A_1,A_2\to B_1,B_2)}_{0,2,SU(d)}(0\|\sigma) = \mathrm{Tr}\, T^{A_1\to A_2\to B^{\otimes 2}}_{inv}\sigma^{\otimes 2} \tag{30}$$

holds. Tsuda *et al.*[1] have obtained a similar result in the two-dimensional case. Thus,

$$\beta^{L(A_1,A_2\to B_1,B_2)}_{0,2,SU(d)}(0\|\sigma) = \beta^{L(A_1,A_2\to B_1,B_2)}_{0,2,SU(d)\times U(1)}(0\|\sigma) = \mathrm{Tr}\, T^{A_1\to A_2\to B^{\otimes 2}}_{inv}\sigma^{\otimes 2}.$$

Therefore, the test $T^{A_1\to A_2\to B^{\otimes 2}}_{inv}$ is a UMP $L(A_1, A_2 \to B_1, B_2)$ G-invariant test with level-0 for the null hypothesis $\mathcal{S}_0$, where $G = SU(d), SU(d)\times U(1)$.

B. n-sample setting

Next, we proceed to n-sample setting. Since the test $T''^n_{\epsilon,\alpha} \stackrel{\rm def}{=} T^n_\alpha(T^{1,A\to B}_{inv}, \frac{d\epsilon}{d+1})$ is level-α $U(d^2-1)$-invariant test with the hypothesis $\mathcal{S}_{\le\epsilon}$, and satisfies the condition of $L(A_1,\ldots,A_n \to B_1,\ldots,B_n)$, the inequality

$$\begin{aligned}&\beta^{L(A_1,\ldots,A_n\to B_1,\ldots,B_n)}_{\alpha,n,U(d^2-1)}(\le \epsilon\|\sigma)\\ \le& {\rm Tr} T''^n_{\epsilon,\alpha}\sigma^{\otimes n} = \beta^n_\alpha\left(\le \frac{d\epsilon}{d+1}\middle\| \frac{dp}{d+1}\right) \end{aligned} \tag{31}$$

holds.

Conversely, as a lower bound of $\beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,SU(d)}(\le \epsilon\|\sigma)$, we obtain

$$\begin{aligned}&\frac{1}{n}\log\frac{\beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,SU(d)}(0\|\sigma)}{1-\alpha}\\ \ge& \min_{u,u':|\langle u|\overline{u'}\rangle|=1,\|u\|=1}\\ &\int_{SU(d)} \log d\langle gu\otimes\overline{g}u'|\sigma|gu\otimes\overline{g}u'\rangle\nu(dg). \end{aligned}\tag{32}$$

C. Asymptotic setting

Taking the limit in (31), we obtain

$$\begin{aligned}&\lim \beta^{L(A_1,\ldots,A_n\to B_1,\ldots,B_n)}_{\alpha,n,U(d^2-1)}\left(\le \frac{\delta}{n}\middle\|\sigma_n\right)\\ \le&\beta_\alpha\left(\le\frac{d\delta}{d+1}\middle\|\frac{dt'}{d+1}\right)\end{aligned}\tag{33}$$

if $\langle\phi^0_{A,B}|\sigma|\phi^0_{A,B}\rangle = 1-\frac{t'}{n}$. Conversely, by using the inequality (32), the compactness of the sets $\{u,u'||\langle u|\overline{u'}\rangle| = 1, \|u\|=1\}$ and $SU(d)$ yields

$$\begin{aligned}&\lim\log\frac{\beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,SU(d)}(0\|\sigma_n)}{1-\alpha}\\ \ge& \min_{u,u':|\langle u|\overline{u'}\rangle|=1,\|u\|=1}\int_{SU(d)}\lim n\\ &\log d\langle gu\otimes\overline{g}u'|\sigma_n|gu\otimes\overline{g}u'\rangle\nu(dg)\\ =&-\min_{u,u':|\langle u|\overline{u'}\rangle|=1,\|u\|=1}\int_{SU(d)}\\ &\lim n\left(1-d\langle gu\otimes\overline{g}u'|\sigma_n|gu\otimes\overline{g}u'\rangle\right)\nu(dg)\\ =&-\min_{u,u':|\langle u|\overline{u'}\rangle|=1,\|u\|=1}\lim n\,{\rm Tr}(I-T_{u,u'})\sigma_n,\end{aligned}$$

where

$$T_{u,u'} \stackrel{\rm def}{=} \int_{SU(d)} d|gu\otimes\overline{g}u'\rangle\langle gu\otimes\overline{g}u'|\nu(dg).$$

Since $T_{u,u'}$ is $SU(d)$-invariant. The test $T_{u,u'}$ has the form $t_0|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}| + t_1(I-|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|)$. The condition $|\langle u|\overline{u'}\rangle| = 1$ guarantees that $t_0 = 1$. The definition of $T_{u,u'}$ guarantees that ${\rm Tr}\,T_{u,u'} \ge d$, which implies $t_1 \ge \frac{1}{d+1}$. Hence,

$$\begin{aligned}&{\rm Tr}(I-T_{u,u'})\sigma_n \le \frac{d}{d+1}{\rm Tr}(I-|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|)\sigma_n\\ =&\frac{d}{d+1}(1-\langle\phi^0_{A,B}|\sigma|\phi^0_{A,B}\rangle) = \frac{d}{d+1}\frac{t'}{n}.\end{aligned}\tag{34}$$

Thus, we have

$$\lim\log\frac{\beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,SU(d)}(0\|\sigma_n)}{1-\alpha} \ge -\frac{dt'}{d+1},$$

which implies

$$\lim\beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,SU(d)}(0\|\sigma_n) \ge (1-\alpha)e^{-\frac{dt'}{d+1}}.$$

Combining (33) in the case of ϵ, we obtain

$$\lim\beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,G}(0\|\sigma_n) = (1-\alpha)e^{-\frac{dt'}{d+1}}$$

for $G = SU(d), SU(d)\times U(1), U(d^2-1)$, $C = S(A_1,\ldots,A_n,B_1,\ldots,B_n), L(A_1,\ldots,A_n,B_1,\ldots,B_n), L(A_1,\ldots,B_1,\ldots,B_n)$. Since $(1-\alpha)e^{-\frac{dt'}{d+1}} < (1-\alpha)e^{-t'} = \beta_\alpha(0\|t')$, there is an advantage to use of quantum correlation among samples.

VIII. TWO-SAMPLE TWO-DIMENSIONAL SETTING

Next, we proceed to the special case $n=2$ and $d=2$. For the analysis of this case, we define the 3×3 real symmetric matrix $V = (v_{i,j})_{1\le i,j\le 3}$ as

$$\begin{aligned}&v_{i,j} \stackrel{\rm def}{=} \Re\langle\phi^i_{A,B}|\sigma|\phi^j_{A,B}\rangle\\ &\phi^1_{A,B} \stackrel{\rm def}{=} \frac{1}{\sqrt{2}}(|10\rangle+|10\rangle),\quad \phi^2_{A,B} \stackrel{\rm def}{=} \frac{1}{\sqrt{2}}(-i|10\rangle+i|10\rangle),\\ &\phi^3_{A,B} \stackrel{\rm def}{=} \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle).\end{aligned}$$

When σ satisfies the following condition $p \le \frac{1}{2}$. the equation

$$\begin{aligned}&\beta^C_{0,2,SU(2)\times U(1)}(0\|\sigma)\\ =&(1-p)^2+\frac{p^2}{3}-\frac{3}{5}\left({\rm Tr}\frac{I}{3}V^2-({\rm Tr}\frac{I}{3}V)^2\right)\end{aligned}\tag{35}$$

holds, where $C = L(A\to B), L(A\leftrightarrows B), S(A,B)$. Since the quantity ${\rm Tr}\frac{I}{3}V^2-({\rm Tr}\frac{I}{3}V)^2$ is greater than 0, its $\frac{3}{5}$ times give the advantage of this optimal test against the test introduced in subsectionVI B. Hence, this merit vanish if and only if the real symmetric matrix V is constant. In addition, the optimal test T is given as follows. First, we define a covariant POVM

$$M_{op}(dg) \stackrel{\rm def}{=} 4\int_{SU(2)} g^{\otimes 2}|u_{op}\rangle\langle u_{op}|(g^{\otimes 2})^\dagger\nu(dg),$$

where the vector u_{op} is defined as

$$u_{op} \stackrel{\rm def}{=} \frac{1}{2}(|01\rangle_{A_1,A_2} - |10\rangle_{A_1,A_2}) + \frac{\sqrt{3}}{2}(|00\rangle_{A_1,A_2} + |11\rangle_{A_1,A_2}).$$

the relation

$$\beta^C_{0,2,SU(2)\times U(1)}(0\|\sigma) = {\rm Tr}\, T(M_{op})\sigma^{\otimes 2} \quad (36)$$

holds. That is, the test $T(M_{op})$ is the UMP $SU(2)\times U(1)$-invariant C test with the condition $p \le \frac{1}{2}$, where $C = L(A \to B), L(A \leftrightarrows B), S(A,B)$.

On the other hand, the RHS of (30) is calculated as

$$\beta^{L(A_1,A_2\to B_1,B_2)}_{0,2,SU(2)}(0\|\sigma) = \beta^{L(A_1,A_2\to B_1,B_2)}_{0,2,SU(2)\times U(1)}(0\|\sigma)$$
$$= (1-\frac{2}{3}p)^2 - \frac{1}{5}\left({\rm Tr}\frac{I}{3}V^2 - ({\rm Tr}\frac{I}{3}V)^2\right). \quad (37)$$

That is, the quantity $\frac{1}{5}\left({\rm Tr}\frac{I}{3}V^2 - ({\rm Tr}\frac{I}{3}V)^2\right)$ presents the effect of use of classical communication between A_1 and A_2.

IX. TWO DIFFERENT STATES

In section VI, we showed that if we can prepare the two identical states simultaneously and we can perform Bell measurement on this joint system, the asymptotically optimal test can be realized. However, it is a bit difficult to prepare two identical states simultaneously. However, as is discussed in this section, if we can prepare two quantum states independently, even if these are not identical, this Bell measurement is asymptotically optimal.

A. Formulation

Since the state on $\mathcal{H}^{\otimes 2}_{A,B}$ can be described as $\sigma_1 \otimes \sigma_2$, our hypotheses are given as

$$H_0: \ \mathcal{S}^2_{\le\epsilon} \stackrel{\rm def}{=} \left\{ \sigma_1\otimes\sigma_2 \,\middle|\, \begin{array}{l}(1-\langle\phi^0_{A,B}|\sigma_1|\phi^0_{A,B}\rangle)\\ +(1-\langle\phi^0_{A,B}|\sigma_2|\phi^0_{A,B}\rangle) \le \epsilon\end{array}\right\}$$

versus

$$H_1: \ \mathcal{S}^{2c}_{\le\epsilon} \stackrel{\rm def}{=} \left\{ \sigma_1\otimes\sigma_2 \,\middle|\, \begin{array}{l}(1-\langle\phi^0_{A,B}|\sigma_1|\phi^0_{A,B}\rangle)\\ +(1-\langle\phi^0_{A,B}|\sigma_2|\phi^0_{A,B}\rangle) > \epsilon\end{array}\right\}.$$

For any group action G introduced in subsection III B, these hypotheses are invariant for $G\times G$-action defined as

$$\phi \mapsto (g_1\otimes g_2)\phi \quad \forall (g_1,g_2)\in G\times G.$$

When only two particles $\mathcal{H}_{A_1,B_1}\otimes\mathcal{H}_{A_2,B_2}$ are prepared, similarly to subsection III C, we can define the quantities $\beta^C_{\alpha,2,G\times G}(\le \epsilon\|\sigma_1\otimes\sigma_2)$ for the condition $C = \emptyset, S(A,B), L(A \leftrightarrows B), L(A \to B), S(A_1,A_2,B_1,B_2), L(A_1,A_2,B_1,B_2), L(A_1,A_2 \to B_1,B_2)$, in which, "2" means two particles, *i.e.*, there is only one sample of $\sigma_1\otimes\sigma_2$. When n samples $(\sigma_1\otimes\sigma_2)^{\otimes n}$ are prepared, we also define the quantities $\beta^C_{\alpha,2n,G\times G}(\le \epsilon\|\sigma_1\otimes\sigma_2)$ for the condition $C = \emptyset, S(A,B), L(A \leftrightarrows B), L(A \to B), S(A_1,A_2,B_1,B_2), L(A_1,A_2,B_1,B_2), L(A_1,A_2 \to B_1,B_2)$.

B. One-sample setting

In this section, we treat the case of *one – sample* and $\epsilon = 0$ case. In the first step, we focus on the case of $C = \emptyset$. In this case, the relations

$$\beta^{\emptyset}_{0,2,G\times G}(0\|\sigma_1\otimes\sigma_2) = \langle\phi^0_{A,B}\otimes\phi^0_{A,B}|\sigma_1\otimes\sigma_2|\phi^0_{A,B}\otimes\phi^0_{A,B}\rangle = (1-p_1)(1-p_2)$$

hold for $G = \emptyset, U(1), SU(d)\times U(1), U(d^2-1)$, where $p_i = 1-\langle\phi^0_{A,B}|\sigma_i|\phi^0_{A,B}\rangle$.

Next, we focus on the case of $C = L(A\to B), L(A\leftrightarrows B), S(A,B)$. When we use the test $T^{2,A\to B}_{inv}$, the second error is

$$\beta(T^{2,A\to B}_{inv}, \sigma_1\otimes\sigma_2) = (1-p_1)(1-p_2) + \frac{p_1p_2}{d^2-1}.$$

Moreover, the optimal second error can also be calculated as

$$\beta^C_{0,2,G\times G}(0\|\sigma_1\otimes\sigma_2) = (1-p_1)(1-p_2) + \frac{p_1p_2}{d^2-1} \quad (38)$$

for $C = L(A\to B), L(A\leftrightarrows B), S(A,B)$ when $\frac{p_1p_2}{d^2-1} \le (1-p_1)p_2, p_1(1-p_2)$. Hence, the test $T^{2,A\to B}_{inv}$ is the C-UMP G-invariant test. Using the PPT condition, Tsuda *et al.*[1] derived this optimal test in the case of $\sigma_1 = \sigma_2, d = 2$.

Finally, we proceed to the case of $C = L(A_1,A_2\to B_1,B_2), L(A_1,A_2,B_1,B_2), S(A_1,A_2,B_1,B_2)$. When we use the test $T^{1,A_1\to B_1}_{inv}\otimes T^{1,A_2\to B_2}_{inv}$, the second error is

$$\beta(T^{1,A_1\to B_1}_{inv}\otimes T^{1,A_2\to B_2}_{inv}, \sigma_1\otimes\sigma_2) = \left(1-\frac{dp_1}{d+1}\right)\left(1-\frac{dp_2}{d+1}\right).$$

the optimal second error is calculated as

$$\beta^C_{0,2,G\times G}(0\|\sigma_1\otimes\sigma_2) = \left(1-\frac{dp_1}{d+1}\right)\left(1-\frac{dp_2}{d+1}\right), \quad (39)$$

for $G = SU(d), SU(d)\times U(1), U(d^2-1)$. Thus, the test $T^{1,A_1\to B_1}_{inv}\otimes T^{1,A_2\to B_2}_{inv}$ is the C-UMP G-invariant test. Tsuda *et al.*[1] derived this optimal test in the case of $\sigma_1 = \sigma_2, d = 2$.

C. Asymptotic setting

In the small deviation asymptotic setting with n samples, we focus on the case $\epsilon = \frac{\delta}{n}$ and $\frac{t'_i}{n} = 1 - \langle \phi^0_{A,B} | \sigma'_{i,n} | \phi^0_{A,B} \rangle$.

$$\lim \beta^{\emptyset}_{\alpha,2n,G\times G}(\le \frac{\delta}{n} \|\sigma'_{1,n} \otimes \sigma'_{2,n}) = \beta_\alpha(\le \delta \|t'_1 + t'_2) \tag{40}$$

for $G = U(1), SU(d) \times U(1), U(d^2-1)$.

Next, we consider the case of $C = L(A \to B)$. When we perform the test $T^{2,A\to B}_{inv}$ for all systems $\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}, \ldots, \mathcal{H}_{A_n} \otimes \mathcal{H}_{B_n}$ whose state is $\sigma'_{1,n} \otimes \sigma'_{2,n}$, the number k of detecting $T^{2,A\to B}_{inv}$ almost obeys the Poisson distribution $e^{-(t'_1+t'_2)} \frac{(t'_1+t'_2)^k}{k!}$. This is because $n\left(1 - (1-\frac{t'_1}{n})(1-\frac{t'_2}{n}) + \frac{\frac{t'_1}{n}\frac{t'_2}{n}}{d^2-1}\right) \to t'_1 + t'_2$. Treating the hypothesis testing of this Poisson distribution, we can show that the $L(A \to B)$ $U(d^2-1) \times U(d^2-1)$-invariant test $T^{n,2}_{c,\alpha} \stackrel{\text{def}}{=} T^n_\alpha(T^{2,A\to B}_{inv}, \max_{p_1+p_2=\epsilon} p_1 + p_2 - \frac{d^2 p_1 p_2}{d^2-1})$ satisfies that

$$\lim \beta(T^{n,2}_{\delta/n,\alpha}, \sigma'_{1,n} \otimes \sigma'_{2,n}) = \beta_\alpha(\le \delta \|t'_1 + t'_2).$$

Hence, combining (40), we obtain

$$\lim \beta^C_{\alpha,2n,G\times G}\left(\le \frac{\delta}{n} \left\| \sigma'_{1,n} \otimes \sigma'_{2,n}\right.\right) = \beta_\alpha(\le \delta \|t'_1 + t'_2).$$

for $C = \emptyset, L(A \to B), L(A \leftrightarrows B), S(A,B)$, $G = SU(d) \times U(1), U(d^2-1)$. Therefore, the test $T^{n,2}_{\epsilon,\alpha}$ is C-UMP G-invariant test in the asymptotic small deviation setting.

Moreover, if we use the test based on the Bell measurement in stead of the test $T^{2,A\to B}_{inv}$, the bound $\beta_\alpha(\le \delta \|t'_1 + t'_2)$ can be attained because a lemma similar to Lemma 5 holds.

X. THREE DIFFERENT STATES

Finally, we treat the case of three quantum states are prepared independently. Similarly to section IX A, we put two hypotheses

$$H_0 : \mathcal{S}^3_{\le\epsilon} \stackrel{\text{def}}{=} \left\{ \bigotimes_{i=1}^3 \sigma_i \left| 1 - \sum_{i=1}^3 \langle \phi^0_{A_i,B_i} | \sigma_i | \phi^0_{A_i,B_i} \rangle \le \epsilon \right.\right\}$$

versus

$$H_1 : \mathcal{S}^{3c}_{\le\epsilon} \stackrel{\text{def}}{=} \left\{ \bigotimes_{i=1}^3 \sigma_i \left| 1 - \sum_{i=1}^3 \langle \phi^0_{A_i,B_i} | \sigma_i | \phi^0_{A_i,B_i} \rangle > \epsilon \right.\right\},$$

where the given state is assumed to be $\sigma_1 \otimes \sigma_2 \otimes \sigma_3$. Similarly we define the quantities $\beta^C_{\alpha,3,G\times G\times G}(\le \epsilon \|\sigma_1 \otimes \sigma_2 \otimes \sigma_3)$ for the condition $C = \emptyset, S(A,B), L(A \leftrightarrows B), L(A \to B), L(A_1, A_2, A_3 \to B_1, B_2, B_3), L(A_1, A_2, A_3, B_1, B_2, B_3), S(A_1, A_2, A_3, B_1, B_2, B$ under the similar $G \times G \times G$-invariance.

Similarly to subsection IX B, we focus on the case of $C = L(A \to B), L(A \leftrightarrows B), S(A,B)$ with one sample. In this case, as is mentioned, the GHZ state $|GHZ\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_{A_1} |i\rangle_{A_2} |i\rangle_{A_3}$ plays an important role. Since the $SU(d) \times SU(d) \times SU(d)$-action on $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_{A_3}$ is irreducible, the following is a POVM:

$$\begin{aligned} &M^3_{cov}(dg_1, dg_2, dg_3) \\ \stackrel{\text{def}}{=}& d^3 g_1 \otimes g_2 \otimes g_3 |GHZ\rangle\langle GHZ| (g_1 \otimes g_2 \otimes g_3)^\dagger \\ & \nu(dg_1)\nu(dg_2)\nu(dg_3). \end{aligned}$$

The test $T^{3,A\to B}_{inv} \stackrel{\text{def}}{=} T(M^3_{cov})$ has the form

$$\begin{aligned} &T^{3,A\to B}_{inv} \\ =& P_1 \otimes P_2 \otimes P_3 + \frac{(d+2) P^c_1 \otimes P^c_2 \otimes P^c_3}{(d+1)^3(d-1)} \\ &+ \frac{P_1 \otimes P^c_2 \otimes P^c_3 + P^c_1 \otimes P_2 \otimes P^c_3 + P^c_1 \otimes P^c_2 \otimes P_3}{(d+1)^2(d-1)}, \end{aligned} \tag{41}$$

where $P_i = |\phi^0_{A_i,B_i}\rangle\langle\phi^0_{A_i,B_i}|, P^c_i = I - P_i$. Thus, this test is $U(d^2-1) \times U(d^2-1) \times U(d^2-1)$-invariant. Hence, when we use the test $T^{3,A\to B}_{inv}$, the second error is

$$\begin{aligned} &\beta(T^{3,A\to B}_{inv}, \sigma_1 \otimes \sigma_2 \otimes \sigma_3) \\ =& (1-p_1)(1-p_2)(1-p_3) + \frac{(d+2) p_1 p_2 p_3}{(d+1)^2(d-1)} \\ &+ \frac{p_1 p_2 (1-p_3) + p_1 (1-p_2) p_3 + (1-p_1) p_2 p_3}{(d+1)^2(d-1)}. \end{aligned}$$

Moreover, the optimal second error can be also calculated as

$$\begin{aligned} &\beta^C_{0,3,G\times G\times G}(0 \|\sigma_1 \otimes \sigma_2 \otimes \sigma_3) \\ =& (1-p_1)(1-p_2)(1-p_3) + \frac{(d+2) p_1 p_2 p_3}{(d+1)^2(d-1)} \\ &+ \frac{p_1 p_2 (1-p_3) + p_1 (1-p_2) p_3 + (1-p_1) p_2 p_3}{(d+1)^2(d-1)} \end{aligned} \tag{42}$$

for $C = L(A \to B), L(A \leftrightarrows B), S(A,B)$ when $p_i \le \frac{d-1}{d}$. Hence, the test $T^{3,A\to B}_{inv}$ is the C-UMP G-invariant test.

On the other hand, the case of $C = L(A_1, A_2, A_3 \to B_1, B_2, B_3), L(A_1, A_2, A_3, B_1, B_2, B_3), S(A_1, A_2, A_3, B_1, B_2, B$ Similarly to (39), we can show the optimality of the test $T^{1,A\to B}_{inv} \otimes T^{1,A\to B}_{inv} \otimes T^{1,A\to B}_{inv}$. Moreover, we can derive the same result in the small deviation asymptotic setting with n samples.

XI. DESIGN FOR TESTS

In this paper, we propose several tests. However, these require a infinite-valued measurement on Alice's space,

which is difficult to realize. In this section, we seek finite-valued POVMs on Alice's space realizing the desired test instead of infinite-valued measurements.

A. Design for the test $T_{inv}^{1,A\to B}$

In order to design the test $T_{inv}^{1,A\to B}$, we focus on the concept "symmetric informationally complete POVM (SIC-POVM)". A rank-one POVM $\{p_i|u_i\rangle\langle u_i|\}$ on $\mathcal{H}_A = \mathbb{C}^d$ is called a *symmetric informationally complete POVM (SIC-POVM)*, if it satisfies the following conditions:

$$\begin{aligned} \#\{i\} =& d^2, \\ p_i =& \frac{1}{d} \\ |\langle u_i|u_j\rangle|^2 =& \frac{1}{d+1} \text{ for } i \neq j \end{aligned} \tag{43}$$

Currently, an SIC-POVM analytically is constructed when the dimension d is 2,3[23, 25],4[22, 25],5[25],6[24],7[26], 8[23], or 19[26]. Also, its existence is numerically verified up to $d = 45$[22]. Any SIC-POVM $M_{sic} = \{p_i|u_i\rangle\langle u_i|\}_i$ satisfies

$$T(M_{sic}) = T_{inv}^{1,A\to B}, \tag{44}$$

that is, the test $T_{inv}^{1,A\to B}$ can be realized by an SIC-POVM. Moreover, if a POVM $M = \{M_i\}_i$ on $\mathcal{H}_A$ satisfies

$$T(M) = T_{inv}^{1,A\to B},$$

the inequality

$$\#\{i\} \geq d^2$$

holds. This is because the rank of the operator $T_{inv}^{1,A\to B}$ (which equal d^2) is less than the number of the elements of POVM M_i. Hence, we obtain

$$\min\{\#\{i\}|T(\{M_i\}_i) = T_{inv}^{1,A\to B}\} = d^2$$

if there exists an SIC-POVM on $\mathbb{C}^d$.

However, any SIC-POVM is not a randomized combination of projection valued measures as well as a projection valued measure. Since projection valued measures are more realizable than other POVM, it is more desired to design Alice's POVM as a randomized combination of projection valued measures. For this purpose, we focus on mutually unbiased bases. $d+1$ orthonormal bases $\{\mathcal{B}_1, \ldots, \mathcal{B}_{d+1}\}$ are called mutually unbiased bases (MUB) if

$$|\langle u|v\rangle|^2 = \frac{1}{d}, \forall u \in \mathcal{B}_i, \forall v \in \mathcal{B}_j, i \neq j.$$

The existence of MUB is shown when d is a prime[27] or a prime power[28]. Bandyopadhyay *et al.* gave a more explicit form in these cases [29]. Any mutually unbiased bases $\{\mathcal{B}_1, \ldots, \mathcal{B}_{d+1}\}$ make the POVM $M_{\mathcal{B}_1,\ldots,\mathcal{B}_k}$, *i.e.*,

$$M_{\mathcal{B}_1,\ldots,\mathcal{B}_{d+1}} = \left\{ \frac{1}{d+1} |u_{i,j}\rangle\langle u_{i,j}| \right\}_{i,j},$$

where $\mathcal{B}_j = \{u_{1,j}, \ldots, u_{d,j}\}$. This POVM always produces the desired test $T_{inv}^{1,A\to B}$ as

$$T(M_{\mathcal{B}_1,\ldots,\mathcal{B}_{d+1}}) = T_{inv}^{1,A\to B}. \tag{45}$$

This construction of the test $T_{inv}^{1,A\to B}$ is optimal in the following sense. Let $\{M^j\}$ be the set of projection-valued measures. A randomized combination of $\{M^j\}$, *i.e.*, $M = \sum_j p_j M_j$ satisfies

$$T(M) = T_{inv}^{1,A\to B}. \tag{46}$$

Then,

$$\#\{j\} \geq d+1, \tag{47}$$

which implies the optimality of the POVM consisting of MUB. Hence,

$$\min_{M_j:PVM} \left\{ \#\{j\} \left| T\left(\sum p_j M_j\right) = T_{inv}^{1,A\to B} \right. \right\} = d+1$$

if d is a prime or a prime power.

B. Design for $T_{inv}^{2,A\to B}$

Next, we proceed to the construction of the test $T_{inv}^{2,A\to B}$. Let f be an irreducible action of group G acts to $\mathcal{H}_{A_1} = \mathbb{C}^d$. By regarding $\mathcal{H}_{A_2}$ as the dual space of $\mathcal{H}_{A_1}$, the matrix $f(g)$ can be regarded as an element of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$. Since the irreducibility of the action f guarantees that

$$\begin{aligned} &\frac{d}{|G|} \sum_{g\in G} \langle k|f(g)|l\rangle\langle l'|f(g)|k'\rangle \\ =& \langle k| \left(\frac{d}{|G|} \sum_{g\in G} f(g)|l\rangle\langle l'|f(g) \right) |k'\rangle \\ =& \langle k|\langle l|l'\rangle I|k'\rangle = \delta_{k,k'}\delta_{l,l'}, \end{aligned}$$

we obtain

$$\begin{aligned} &\frac{d}{|G|} \sum_{g\in G} \left| \left\langle \sum_{k,l} a_{k,l} E_{k,l} \right| f(g) \right\rangle \Big|^2 \\ =& \frac{d}{|G|} \sum_{g\in G} \sum_{k,l} \sum_{k',l'} a_{k,l}\overline{a_{k',l'}} \langle k|f(g)|l\rangle\langle l'|f(g)|k'\rangle \\ =& \sum_{k,l} a_{k,l}\overline{a_{k,l}}, \end{aligned}$$

which implies

$$\frac{d^2}{|G|}\sum_{g\in G}\left|\frac{1}{\sqrt{d}}f(g)\right\rangle\left\langle\frac{1}{\sqrt{d}}f(g)\right| = I_{A_1,A_2}.$$

Hence, $M_f = \left\{\frac{d^2}{|G|}\left|\frac{1}{\sqrt{d}}f(g)\right\rangle\left\langle\frac{1}{\sqrt{d}}f(g)\right|\right\}_{g\in G}$ is a POVM.

Furthermore, we assume that the action $f\otimes\overline{f}$ of G to $\mathcal{H}_{A_1}\otimes\mathcal{H}_{A_2}$ has only two irreducible components, *i.e.*, the irreducible subspaces of $\mathcal{H}_{A_1}\otimes\mathcal{H}_{A_2}$ are only the one-dimensional space $<\phi^0_{A_1,A_2}>$ and its orthogonal space $<\phi^0_{A_1,A_2}>^{\perp}$. In this case, The test $T(M_f)$ satisfies

$$T(M_f) = T^{2,A\to B}_{inv}. \tag{48}$$

In particular, the action of Clifford group on $\mathbb{C}^d$ satisfies this condition when d is prime[26]. Hence, we can construct a finite-valued POVM producing the test $T^{2,A\to B}_{inv}$.

XII. CONCLUSION

In this paper, we treated the hypotheses testing problem when the null hypothesis consists only of the required entangled state or is its neighboor hood. In order to treat the structure of entanglement, we consider three settings concerning the range of accessible measurements as follows: **M1**: All measurement is allowed. **M2**: A measurement is forbidden if it requires the quantum correlation between two distinct parties. **M3**: A measurement is forbidden if it requires the quantum correlation between two distinct parties, or that among local samples. As a result, we found that there is difference between the accuracies of **M1** and **M2** in the first order asymptotics. The protocol achieving the asymtotic bound has been proposed in the setting **M2**. In this setting, it is required to prepare two identical samples at the same time. However, it is difficult to keep their coidentity. In order to avoid this difficulity, we proved that even if they do not coninicide, this proposed protocol works effectively. In particular, this protocl can be realized in the two-dimensional system if the four-valued Bell measurement can be realized. Moreover, concerning the finite samples case, we derived optimal testing in several examples.

In this paper, the optimal test is constructed based on continuous valued POVM. However, any realizable POVM is finite valued.

The obtained protocol is essentially equivalent with the following procedure based on the quantum teleportation. Fisrt, we perform quantum teleportation from the system A to the system B, which succeed when the ture state is the required maximally entangled state. Next, we check whether the state on the system B is the initial state on the system A. Hence, an interesting relation between the obtained results and the quantum teleportation is expected, and it will be treated in another forcoming paper [33].

As a related research, the following testing problem has been discussed [30, 31]. Assume that N qubits state are given, and we can measure only M qubits. The required problem is testing whether the remaining $N-M$ qubits are the desired maximally entangled state. Indeed, this problem is important not only for gurarantee of the quality of the prepared maximally entangled state, but also for the security for the quantum key distribution. The problem discussed in this paper is different from the preceding probelem in testing the given state by measuring the whole system. In order to apply our result to the preceding problem, we have to ramdomly choose M qubits among the given N qubits, and test the N qubits. When the given N qubits do not satisfy the independent and identical condition, their method [30, 31] is better than our method. Since their method [30, 31] requires the the quantum correlation among whole M qubits, it is difficult to realize their method for testing the prepared maximally entangled state, but it is possible to apply their method to testing the security of quantum key distribution [30]. This is because the maximally entangled state is only virtually discussed in the latter case. Hence, for testing the prepared maximally entangled state, it is natual from the practical viewpoint to restrict our test among ramdom sampling method. Since our results can be applied this setting, they can be expected to be applied to the check of the quality of maximally entangled state.

As another problem, Acín *et al.* [5] discussed the problem testing whether the given n-i.i.d. state of the unkown pure state is the n-tensor product of a pure maximally entangled state (not the specific maximally entangled state) in the two-dimensional system. Its d-dimensional case is discussed in Matsumoto and Hayashi [32], and this problem is closely related to universal entanglement concentration.

This problem is different from our setting, but is very important. Hence, it is needed to discuss this setting with the mixed state case.

[1] Y. Tsuda, M. Hayashi, and K. Matsumoto, "Hypothesis Testing for Entanglement," *Proc. of EQIS'05*, pp. 70-71, (2005).

[2] A. S. Holevo, "Covariant measurements and uncertainty relations," *Rep. Math. Phys.*, **16**, 385-400, (1979).

[3] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, (North-Holland, Amsterdam, 1982).

[4] M. Hayashi eds., *Asmptotic Theory of Quantum Statistical Inference: Selected Papers*, (World Scientific, Singapore, 2005).

[5] A. Acin, R. Tarrach, and G. Vidal "Optimal estimation of two-qubit pure-state entanglement," *Phys. Rev. A* **61**, 62307, (2000).

[6] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.* **70** 1895, (1993).

[7] C. Bennett, and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.* **69** 2881, (1992).

[8] G. M. D'Ariano, C. Macchiavello, and M. G. A. Paris, "Local observables for entanglement witnesses," *Phys. Rev. A* **67** 042310, 2003.

[9] A. Ekert, *Phys. Rev. Lett.* **67** 661, 1991.

[10] Gühne, O., Hyllus, P., Brus, D., Ekert, A., Lewenstein, M., Macchiavello, C. and Sanpera, A. "Detection of entanglement with few local measurements," *Phys. Rev. A* **66** 062305, 2002.

[11] M. Hayashi, "Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing," *J. Phys. A* **35** 10759-10773, (2002).

[12] C. W. Helstrom, *Quantum detection and estimation theory* (Academic Press, 1976).

[13] F. Hiai, and D. Petz, "The proper formula for relative entropy and its asymptotics in quantum probability," *Comm. Math. Phys.*, **143**, 99-114, (1991).

[14] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).

[15] E. L. Lehmann, *Testing statistical hypotheses* Second edition. (Wiley, 1986).

[16] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, *Phys. Rev. A* **62** 052310, (2000).

[17] E.M. Rains, *Phys. Rev. A*, **60**, 173 (1999).

[18] E.M. Rains, *IEEE Trans. Inf. Theory* **47**, 2921 (2001).

[19] B. M. Terhal, "Bell Inequalities and the Separability Criterion," *Phys. Lett. A* **271** 319, (2000).

[20] T. Ogawa, and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing," *IEEE Trans. Inform. Theory* **46** 2428-2433, (2000).

[21] S. Virmani, and M. B. Plenio, "Construction of extremal local positive-operator-valued measures under symmetry," *Phys. Rev. A* **67** 062308, (2003).

[22] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, "Symmetric Informationally Complete Quantum Measurements," *J. Math. Phys.*, **45**, 2171-2180 (2004); quant-ph/0310075.

[23] A. Koldobsky and H. König, "Aspects of the Isometric Theory of Banach Spaces," in *Handbookof Geometry of Banach Spaces*, Vol. 1, edited by W. B. Johnson and J. Lindenstrauss (North-Holland, Dordrecht, 2001), pp.899-939.

[24] Grassl, M., "On SIC-POVMs and MUBs in dimension 6," *Proceedings of EQIS'04*, pp. 60-61, (2004); quant-ph/0406175.

[25] Zauner, G., "Quantum designs—foundations of a noncommutative theory of designs," (in German), Ph.D. thesis, University of Vienna, (1999).

[26] Appleby, D M, "SIC-POVMs and the Extended Clifford Group," quant-ph/0412001.

[27] I. D. Ivanovic, "Geometrical description of quantum state determination," *Journal of Physics A*, **14**, No. 12, 3241-3245, (1981).

[28] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Annals of Physics*, **191**, No. 2, 363-381, (1989).

[29] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, "A New Proof for the Existence of Mutually Unbiased Bases," Algorithmica, 34 (2002), pp. 512-528; quant-ph/0103162.

[30] Lo, H.-K. and Chau, H. F., "Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances," *Science*, **283**, 2050 (1999); quant-ph/9803006.

[31] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, "Mixed State Entanglement and Quantum Error Correction," *Phys. Rev. A*, **54**, 3824 (1996); quant-ph/9604024.

[32] K. Matsumoto and M. Hayashi, quant-ph/0109028.

[33] M. Hayashi, in preparation.